On the groups of codes with empty kernel

Jean Berstel, Clelia De Felice, Dominique Perrin, Giuseppina Rindone

On the groups of codes with empty kernel

Jean Berstel[1], Clelia De Felice[2], Dominique Perrin[1] and Giuseppina Rindone[1]
[1]Université Paris Est, LIGM, 77454 Marne-la-Vallée France,
[2]Università degli Studi di Salerno, via Ponte Don Melillo, Fisciano (SA) 84084 Italy

February 19, 2010

Abstract

An internal factor of a word x is a word v such that $x = uvw$ for some nonempty words u, w. The *kernel* of a set X of words is the set of words of X which are internal factors of words of X. Let φ be the syntactic morphism of the submonoid X^* generated by X. We prove that if X is a code with empty kernel, the groups contained in the image by φ of the complement of the set of internal factors of the words of X are cyclic. This generalizes a result announced by Schützenberger in 1964.

1 Introduction

Groups contained in finite monoids play an important role in their description. In particular, the finite monoids containing only groups in a given variety of finite groups form a variety of finite monoids. These varieties have been studied in several cases including the trivial variety of groups, corresponding to the variety of aperiodic monoids. The study of groups contained in syntactic monoids of sets of words is an important chapter of automata theory. To a given variety of finite monoids corresponds a family of rational sets called a $*$-variety(see [2] or [4] for an introduction to this subject). We will prove here results which show that the groups in the syntactic monoids of some sets are cyclic and thus belong to the variety of Abelian groups.

We actually prove here a result (Theorem 1 below) which is a generalization of the fact that the group of a semaphore code is cyclic. The starting point of this research is the article *On the synchronizing properties of certain prefix codes* published by Schützenberger in 1964 [5]. This paper presents a family of maximal prefix codes called $\mathcal{J}$-codes, that we call *semaphore codes*. The main result of [5] is that a semaphore code is always of the form X^n where X is a synchronized semaphore code and $n \geq 1$. Two proofs are presented of this result in [5]. The first one is combinatorial and rather hard to follow. The second one uses intermediary results which are interesting in their own (this is the proof presented in [1]). First, it is proved ([5], Remark 1) that the group of a semaphore code is a regular permutation group. Next, it is proved ([5], Property 2) that if the group G of a maximal prefix code X is regular (the statement says Abelian but the proof uses only the fact that it is regular), then there is a decomposition $X = Y \circ Z \circ T$ such that Y, T are synchronizing and Z is a group code with $G(Z) = G$. A third result ([5], Remark 2) shows that if X is a semaphore code such that $X = Y \circ Z \circ T$ with Z a regular group code, then $X = U^n$ with U a synchronized semaphore code and $n \geq 1$. This implies that the group of a semaphore code is cyclic since $G(U)$

is trivial and $G(X) = \mathbb{Z}/n\mathbb{Z}$. At the end of the paper, it is claimed that all groups in the syntactic monoid of X^* which are not included in the image of the set of factors of X are cyclic, but the proof is not correct.

We prove here a generalization replacing semaphore codes by codes with empty kernel. An internal factor of a word x is a word v such that $x = uvw$ for some nonempty words u, w. The kernel of a set of words $X \subset A^+$ is the set of words of X which are internal factors of words of X. In particular, a semaphore code has empty kernel but codes with empty kernel are more general since they need not be prefix nor maximal. Let X be a code with empty kernel and let F be the set of internal factors of words of X. Let φ be the morphism from A^* onto the transition monoid of an unambiguous automaton $\mathcal{A} = (Q, 1, 1)$ recognizing X^*. We prove that any group G contained in $\varphi(A^* \setminus F)$ is cyclic (Theorem 1). We deduce from this result a closure property of the $*$-variety corresponding to the variety of monoids containing only Abelian groups (Theorem 2).

The article is organized as follows. In the first section, we introduce preliminary results and recall some definitions about codes and unambiguous automata. We prove in particular a result on sets of interpretations of a word with respect to a code with empty kernel (Lemma 2). In Section 3, we prove the main result (Theorem 1) and list some corollaries. We illustrate these results on several examples. They were computed with the help of the software Semigroupes [3] available at `http://www.liafa.jussieu.fr/~jep/Semigroupe2.0/semigroupe2.html`. In the last section, we use Theorem 1 to prove a closure property of the $*$-variety $\mathcal{V}$ of recognizable sets such that their syntactic monoid contains only Abelian groups. In fact, we prove that if X is a code with empty kernel which is in $\mathcal{V}$, then X^* is also in $\mathcal{V}$ (Theorem 2).

2 Preliminaries

In this section, we introduce the notions used in the paper. For a more detailed exposition, see [1].

2.1 Codes and interpretations

Let A be a finite alphabet. We denote by A^* the free monoid on A and by A^+ the free semigroup on A. The empty word is denoted by 1.

Codes. A *code* is a set $X \subset A^+$ such that $x_1 \cdots x_n = y_1 \cdots y_m$ with $x_i, y_j \in X$ implies $n = m$ and $x_i = y_i$ for $1 \leq i \leq n$.

When $X \subset A^+$ is a code, the submonoid X^* generated by X is *stable*. This means that, for any words u, v, w in A^*, if u, uv, vw and w are in X^* then v is also in X^*.

A set $X \subset A^*$ is said to be *dense* if any word in A^* is a factor of a word in X. A set which is not dense is said to be *thin*. A set $X \subset A^*$ is *complete* if X^* is dense.

A *prefix code* is a set $X \subset A^+$ such that no word of X is a prefix of another word of X. The definition of a suffix code is symmetrical. A *bifix code* is a set which is simultaneously a prefix code and a suffix code.

An *infix code* is a set $X \subset A^+$ such that no word of X is a factor of another word of X.

A *semaphore code* is a set of the form $A^*S \setminus A^*SA^+$ for some nonempty set $S \subset A^+$. A semaphore code is prefix by definition. Conversely, it can be shown that a prefix code $X \subset A^+$ is a semaphore code if and only if $A^*X \subset XA^*$. A semaphore code is thin and complete.

For any semaphore code $X \subset A^+$, the set $Y = X \setminus A^*X$ is an infix code.

An *internal factor* of a word $x \in A^*$ is a word $v \in A^*$ such that $x = uvw$ for some nonempty words u, w. The *kernel* of a set of words $X \subset A^+$ is the set of words of X which are internal factors of words of X.

Examples of codes with empty kernel include infix codes and semaphore codes.

Factorizations. A *factorization* of a word $w \in A^*$ is a sequence $(u_1, u_2, \ldots, u_n)$ with $n \geq 1$, $u_i \in A^+$ for $2 \leq i \leq n-1$ and $u_1, u_n \in A^*$ such that $w = u_1 u_2 \cdots u_n$. Thus the terms of a factorization are all nonempty, except possibly the first and the last one.

The *content* of a sequence $\alpha = (u_1, u_2, \ldots, u_n)$ of words $u_i \in A^*$ is the word $w = u_1 u_2 \cdots u_n$. We denote $w = c(\alpha)$.

For a factorization $\alpha = (u_1, u_2, \ldots, u_n)$, we denote

$$P(\alpha) = \{u_1, u_1u_2, \ldots, u_1u_2 \cdots u_{n-1}\}.$$

We say that β *refines* α, denoted $\alpha < \beta$, if $P(\alpha) \subset P(\beta)$. The *supremum* of two factorizations $\alpha = (u_1, u_2, \ldots, u_n)$ and $\beta = (v_1, v_2, \ldots, v_m)$ of a word w, denoted $\alpha \vee \beta$, is the unique factorization $\gamma = (w_1, w_2, \cdots, w_p)$ of w such that $P(\gamma) = P(\alpha) \cup P(\beta)$.

Example 1 The word $w = ab$ has 8 distinct factorizations represented in Figure 1 with the refinement order indicated vertically.

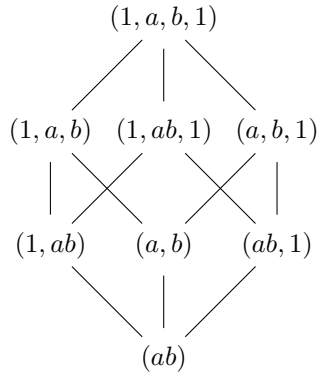

Figure 1: The 8 factorizations of $w = ab$.

Two factorizations α and β of a word w are *adjacent* if $P(\alpha) \cap P(\beta) \neq \emptyset$. Thus $\alpha = (u_1, u_2, \ldots, u_n)$ and $\beta = (v_1, v_2, \ldots, v_m)$ are adjacent if there exists i, j with $1 \leq i < n$ and $1 \leq j < m$ such that $u_1 \cdots u_i = v_1 \cdots v_j$ and $u_{i+1} \cdots u_n = v_{j+1} \cdots v_m$. Two factorizations which are not adjacent are *disjoint*.

Interpretations. Let $X \subset A^+$ be a code. Let P be the set of proper prefixes of the words of X and let S be the set of proper suffixes of the words of X. An *interpretation* of a word $w \in A^*$ with respect to X is a factorization $\alpha = (s, x_1, x_2, \ldots, x_n, p)$ of w such that $s \in S$, $n \geq 0$, $x_i \in X$ and $p \in P$.

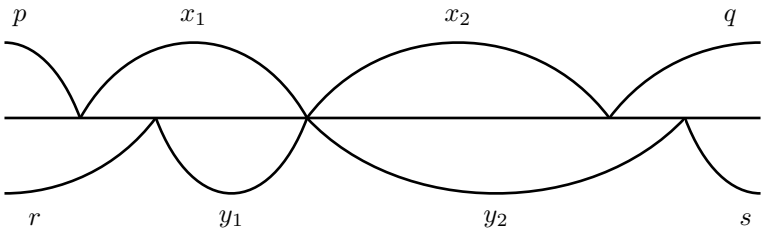

Figure 2: Two adjacent interpretations

Thus an interpretation α is made of three parts: a proper suffix s of X denoted s_α, a possibly empty sequence $(x_1, x_2, \cdots, x_n)$ of words of X denoted f_α and a proper prefix p of X denoted p_α. In particular, an interpretation is a factorization with at least two terms.

Two interpretations of a word w are said to be adjacent (resp. disjoint) if the corresponding factorizations are adjacent (resp. disjoint) (see Figure 2).

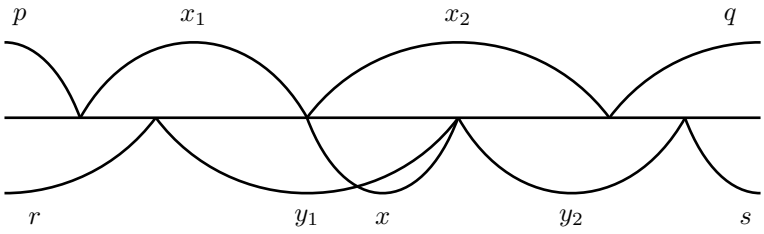

Figure 3: Two connected interpretations

Two interpretations α, β of a word w are *connected* if $w = uxv$ for some words $u, v \in A^*$ and $x \in X^*$ such that $u \in P(\alpha)$ and $ux \in P(\beta)$.

Note that α, β are connected if and only if there exists an interpretation γ of w which is adjacent to α and β (see Figure 3). Thus adjacent interpretations are connected. The converse is not true in general as shown by the following example.

Example 2 Let $A = \{a, b\}$ and let $X = \{aab, bbb, bba, baa, aabbb\}$. The word $w = aabbba$ has two disjoint interpretations $\alpha = (aa, bbb, a)$ and $\beta = (1, aab, bba, 1)$. They are connected since both are adjacent to $\gamma = (1, aabbb, a)$.

Two interpretations of a word which are not connected are said to be *independent*.

For each set of interpretations of a word w, one may consider their supremum, which is a factorization of w. Let $(u_1, u_2, \ldots, u_m)$ be the supremum of a set I of interpretations of a word w. Then for each k with $1 \leq k < m$ there is an element of I which refines the factorization $(u_1 \cdots u_k, u_{k+1} \cdots u_m)$.

Residuals. For a word $u \in A^*$ and a set $X \subset A^*$, we denote $u^{-1}X = \{v \in A^* \mid uv \in X\}$. In particular, when $X = \{w\}$ has just one element, we write $u^{-1}w$ instead of $u^{-1}\{w\}$. If $u^{-1}w$ is not empty, we identify the set $u^{-1}w$ with the word v such that $w = uv$.

For a letter $a \in A$ and a sequence $\alpha = (u_1, u_2, \ldots, u_n)$ of words $u_i \in A^*$, we define a sequence of words $a^{-1}\alpha$ as follows. First $a^{-1}\alpha = \emptyset$ if $n = 0$. Next, for $n \geq 1$, we define by induction on n

$$a^{-1}\alpha = \begin{cases} a^{-1}(u_2, \ldots, u_n) & \text{if } u_1 = 1 \\ (a^{-1}u_1, u_2, \ldots, u_n) & \text{if } u_1 \in aA^* \\ \emptyset & \text{otherwise.} \end{cases}$$

Let α be a factorization of a word $w \in A^+$ and let $a \in A$ be a letter. Then $a^{-1}\alpha$ and $a^{-1}w$ are nonempty if and only if a is the first letter of w. In this case $a^{-1}\alpha$ is a factorization of $a^{-1}w$.

Example 3 We have already seen that the word $w = ab$ has 8 distinct factorizations (Example 1) represented in Figure 4 on the left with the refinement order. The 4 distinct factorizations of the word $a^{-1}w = b$ are represented on the right.

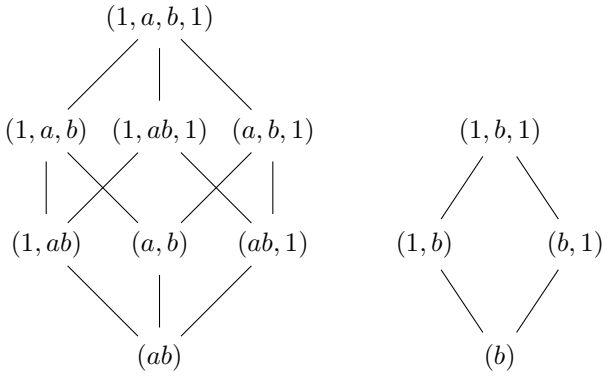

Figure 4: The 8 factorizations of $w = ab$ and the 4 factorizations of $a^{-1}w = b$.

Let α be an interpretation of a nonempty word $w \in A^+$ with respect to a code X and let a be the first letter of w. Suppose that $s_\alpha \neq 1$ or that f_α is not empty. Then $a^{-1}\alpha$ is an interpretation of $a^{-1}w$. Indeed, let $\alpha = (s, x_1, x_2, \ldots, x_n, p)$. If $s \neq 1$, then $a^{-1}\alpha = (a^{-1}s, x_1, x_2, \ldots, x_n, p)$. Next, if $s = 1$ and $n \geq 1$, then $a^{-1}\alpha = (a^{-1}x_1, x_2, \ldots, x_n, p)$.

Lemma 1 *Let α, β, be two independent interpretations of a nonempty word w. Let a be the first letter of w and let $w' = a^{-1}w$, $\alpha' = a^{-1}\alpha$, $\beta' = a^{-1}\beta$. We assume that $s_\alpha \neq 1$ or f_α is not empty and that $s_\beta \neq 1$ or f_β is not empty. Then α', β' are independent interpretations of w'.*

Proof. The condition guarantees that α' and β' are interpretations of w'. Suppose that α', β' are connected. Let $u, v \in A^*$ and $x \in X^*$ be such that $w' = uxv$ with $u \in P(\alpha')$ and $ux \in P(\beta')$. Then $w = auxv$ with $au \in P(\alpha)$ and $aux \in P(\beta)$ implies that α and β are connected, a contradiction. ∎

Let I be a set of n interpretations of a word w. Let $(u_1, u_2, \ldots, u_m)$ be the supremum of the elements of I. For $\alpha \in I$, set $w = sxp$ with $s = s_\alpha$, $x = c(f_\alpha)$ and $p = p_\alpha$. There are unique integers i, j with $1 \leq i \leq n$ and $i \leq j < m$ such that

$$s = u_1 \cdots u_i, \quad x = u_{i+1} \cdots u_j, \quad p = u_{j+1} \cdots u_m. \tag{1}$$

We define

$$\lambda(\alpha, I) = i - 1, \quad \mu(\alpha, I) = j - i, \quad \nu(\alpha, I) = m - j - 1. \tag{2}$$

Thus $\lambda(\alpha, I), \mu(\alpha, I)$ and $\nu(\alpha, I)$ are the number of words u_k which compose each element of the interpretation, not taking in account the (possibly empty) first and last one.

A factorization $(u_1, u_2, \ldots, u_m)$ of a word w is said to be *n-periodic* with respect to a code X if for any r, ℓ with $1 \leq \ell \leq r \leq m - 1$, one has $u_{\ell+1} \cdots u_r \in X$ if and only if $r - \ell = n$. Thus, in other terms, the factorization is n-periodic if and only if the number of consecutive nonempty factors u_i with $2 \leq i \leq m - 1$ whose product is in X is constant and equal to n.

A set I of n interpretations of a word w with respect to a code X is said to be *cyclic* if the supremum $(u_1, u_2, \ldots, u_m)$ of the n interpretations is n-periodic with respect to X (see Figure 5).

Let I be a set of n interpretations of a word w with respect to a code X. If I is cyclic, then for each $\alpha \in I$,

$$\mu(\alpha, I) \equiv 0 \mod n \tag{3}$$

Indeed, let $\sigma = (u_1, u_2, \ldots, u_m)$ be the supremum of the elements of I. Since I is cyclic, the factorization σ is n-periodic. Thus, each word of X which appears in the content of f_α is a product of n consecutive nonempty elements of σ.

Note that if the set I is cyclic, the elements of I are pairwise independent. Let indeed $(u_1, \ldots, u_m)$ be the supremum of the elements of I. Let α be an element of I and set $s_\alpha = u_1 \cdots u_i$ with $1 \leq i < n$. Then for $i \leq r \leq m - 1$, $u_1 \cdots u_r \in P(\alpha)$ implies $u_{i+1} \cdots u_r \in X^*$ and thus $r \equiv i \mod n$. Thus $u_1 \cdots u_r \in P(\alpha)$ implies $r - 1 \equiv \lambda(\alpha, I) \mod n$.

Let then $\alpha, \beta \in I$ be connected. By definition, we have $w = uxv$ for some words $u, v \in A^*$ and $x \in X^*$ such that $u \in P(\alpha)$ and $ux \in P(\beta)$. Set $u = u_1 \cdots u_\ell$ and $x = u_{\ell+1} \cdots u_r$. Then, by the above argument, we have $\lambda(\alpha, I) \equiv \ell - 1 \mod n$ and $\lambda(\beta, I) \equiv r - 1 \mod n$. Since $x \in X^*$, we have also $r - \ell \equiv 0 \mod n$. Finally, we obtain $\lambda(\alpha, I) \equiv \lambda(\beta, I) \mod n$ and thus $\lambda(\alpha, I) = \lambda(\beta, I)$. In the same way $\nu(\alpha, I) = \nu(\beta, I)$ and thus $\alpha = \beta$.

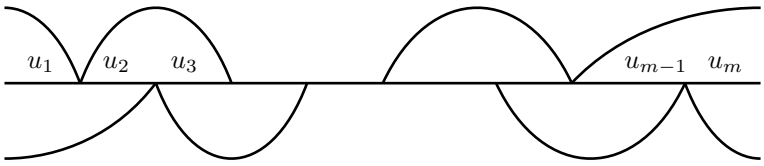

Figure 5: A cyclic set of two interpretations

Example 4 Let $A = \{a, b\}$ and $X = \{aab, abaa, abab, baba\}$. The set X is a code with empty kernel. The word $w = ababaababa$ has the set I of 3 interpretations $(1, abab, aab, aba)$, $(a, baba, abab, a)$ and $(ab, abaa, baba, 1)$. The supremum of these interpretations is the 3-periodic factorization $(1, a, b, ab, a, a, b, ab, a, 1)$ of w with $m = 10$ factors. Thus I is cyclic.

We will use the following result.

Lemma 2 *Let $X \subset A^+$ be a code with empty kernel. Any set of independent interpretations of a word with respect to X is cyclic.*

Proof. Let w be a word with n pairwise independent interpretations. The proof is by induction on the length of w. It is true for the empty word since in this case there is at most one interpretation, which is $(1, 1)$ and the property holds trivially.

Assume that the property holds for the words shorter than a nonempty word w. Let I be a set of n pairwise independent interpretations of w. Set $I = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ in such a way that s_{α_i} is a proper prefix of $s_{\alpha_{i+1}}$ for $0 \leq i \leq n-2$. We first consider the case where $s_{\alpha_0} \neq 1$ or f_{α_0} is not empty.

In this case, set $w = aw'$ with $a \in A$ and $w' \in A^*$. By Lemma 1 the set $I' = \{a^{-1}\alpha \mid \alpha \in I\}$ is a set of n pairwise independent interpretations of w'. By induction hypothesis the set I' is cyclic and the supremum $\mu = (u_1, \ldots, u_m)$ of the elements of I' is n-periodic.

If $s_{\alpha_0} \neq 1$, then the sequence $\nu = (au_1, \ldots, u_m)$ is the supremum of the elements of I. Since ν is also n-periodic, the set I is cyclic.

If $s_{\alpha_0} = 1$ and f_{α_0} is nonempty, the sequence $\nu = (1, au_1, \ldots, u_m)$ is the supremum of the elements of I. We verify that ν is n-periodic. Since $\mu = (u_1, \ldots, u_m)$ is n-periodic, one has $u_{\ell+1} \cdots u_r \in X$ if and only if $r - \ell = n$ for $1 \leq \ell \leq r \leq m-1$.

We have to show that additionally, $au_1u_2 \cdots u_r \in X$ if and only if $r = n$. Let us prove that we cannot have $au_1u_2 \cdots u_r \in X$ with $r < n$. Indeed, since X is a code with empty kernel, no word $x \in X$ can be a proper prefix (or a proper factor) of s_{α_i} for $i \in \{1, \ldots, n-1\}$ (otherwise x would be proper factor of zs_{α_i}, where $z \in A^+$ is such that $zs_{\alpha_i} \in X$). As a consequence, $au_1u_2 \cdots u_r = s_{\alpha_r}$, $r \in \{1, \ldots, n-1\}$ (see also Equation (1)) and $au_1u_2 \cdots u_r = s_{\alpha_r} \notin X$ for $r < n-1$. Furthermore, if $au_1u_2 \cdots u_{n-1} = s_{\alpha_{n-1}} \in X$, $\gamma = (1, s_{\alpha_{n-1}} f_{\alpha_{n-1}}, p_{\alpha_{n-1}})$ would be adjacent to α_0 and to α_{n-1}, a contradiction. Let us prove that we cannot have $au_1u_2 \cdots u_r \in X$ with $r > n$. Notice that $u_2 \cdots u_{n+1} \in X$ (I' is cyclic) and so, $u_2 \cdots u_{n+1}$ is the first term in f_{α_1}. Furthermore, $u_i \neq 1$ for $i \in \{2, \ldots, m-1\}$, since μ is a factorization. Thus, we cannot have $au_1u_2 \cdots u_r \in X$ with $n+1 < r \leq m-1$ since $u_2 \cdots u_{n+1} \in X$ and X is a code with empty kernel and we cannot have $au_1u_2 \cdots u_{n+1} \in X$ since $\gamma = (1, s_{\alpha_1} f_{\alpha_1}, p_{\alpha_1})$ would be adjacent to α_0 and to α_1. Finally, since $au_1u_2 \cdots u_n$ is the first term in the sequence f_{α_0}, we have $au_1u_2 \cdots u_n \in X$.

Suppose finally that $s_{\alpha_0} = 1$ and f_{α_0} is empty. In this case $w = p_{\alpha_0}$ and thus the sequences f_{α_j} for $j \in \{1, \ldots, n-1\}$ are empty. Indeed, otherwise their terms would be proper factors of $p_{\alpha_0}y$, where $y \in A^+$ is such that $p_{\alpha_0}y \in X$ (as $s_{\alpha_j} \neq 1$ for $j \in \{1, \ldots, n-1\}$). Consequently, $\alpha_j = (s_{\alpha_j}, p_{\alpha_j})$, $P_{\alpha_j} = \{s_{\alpha_j}\}$, $0 \leq j \leq n-1$, and the supremum of the set I is $(u_0, \ldots, u_{n-1}, u_n)$, with $u_0 \cdots u_j = s_{\alpha_j}$, $0 \leq j \leq n-1$, and $u_n = p_{\alpha_{n-1}}$. In order to conclude that this factorization is n-periodic we have to prove that $u_0 \cdots u_j = s_{\alpha_j} \notin X$, for $0 < j \leq n-1$. Now, we cannot have $u_0 \cdots u_j = s_{\alpha_j} \in X$, for $0 < j < n-1$, since otherwise $s_{\alpha_j} \in X$ would be proper factor of $zs_{\alpha_{n-1}}$, where $z \in A^+$ is such that $zs_{\alpha_{n-1}} \in X$, nor can we have $u_0 \cdots u_{n-1} = s_{\alpha_{n-1}} \in X$, since otherwise $\gamma = (1, s_{\alpha_{n-1}}, p_{\alpha_{n-1}})$ would be adjacent to α_0 and to α_{n-1}, a contradiction. ∎

Observe that Lemma 2 is not true for a set of disjoint interpretations (instead of independent) as shown by the following example.

Example 5 Let $A = \{a, b\}$ and let $X = \{aab, bbb, bba, baa, aabbb\}$ as in Example 2. The code X has empty kernel. The word $w = aabbba$ has two disjoint interpretations $\alpha = (aa, bbb, a)$ and $\beta = (1, aab, bba, 1)$. The supremum of α, β is the factorization $(1, aa, b, bb, a, 1)$. It is not 2-periodic since $aabbb$ is in X although it is a product of three terms of the factorization.

2.2 Groups, monoids and automata

We now give definitions concerning groups, monoids and automata. Again, for a more detailed presentation, see [1].

Permutation groups. Let us recall some terminology about permutation groups (see also [7]). Let G be a permutation group on a set R. We denote the action of G on R on the right. Thus an element g of G maps each $r \in R$ to some $rg \in R$. The *degree* of G is the cardinality of the set R. The *order* of G is the cardinality of G. The *orbits* of G are the classes of the equivalence on R defined by $p \equiv q$ if there exists $g \in G$ such that $pg = q$. The group G is said to be *transitive* if there is only one orbit.

A permutation group is called *regular* if no element distinct from the identity has a fixpoint. All orbits in a regular group have the same cardinality equal to the order of the group. In particular, the order of a regular group is a divisor of its degree. A finite permutation group is cyclic and regular if and only if it is generated by a permutation composed of disjoint cycles of the same length. As mentionned in the introduction, a transitive permutation group which is Abelian is regular (see [7], Proposition 4.4). Indeed, suppose that $rg = r$ for some $r \in R$ and $g \in G$. Let us show that $sg = s$ for any $s \in R$. Since G is transitive, there is some $h \in G$ such that $r = sh$. Since G is Abelian, $hg = gh$ and thus $shg = sh$ implies $sgh = sh$. Since h is a permutation on R, this implies $sg = s$. Thus g is the identity and this shows that G is regular.

Ideals in monoids. A *group in a monoid* M is a subset G of M such that the operation of M gives to G a group structure. More precisely, a group in M is a subset G of M containing an idempotent e, such that for any $g, h \in G$ one has $gh \in G$ and such that for any $g \in G$ there is some $h \in G$ such that $gh = hg = e$.

For any idempotent e in a monoid M, there is a largest group G contained in M which has e as neutral element, called the *maximal group* containing e. It is the set of all $m \in M$ such that $em = me = m$ and such that there exists $n \in M$ such that $mn = nm = e$.

An *ideal* of a monoid M is a nonempty subset I of M such that for any $m, n \in M$ and $x \in I$, one has $mxn \in I$. If I is an ideal and G is a group contained in M, then either $G \cap I = \emptyset$ or $G \subset I$. Indeed, let $x \in G \cap I$. Then for any $g \in G$, we have $g = x^{-1}xg$ and thus g is in I.

Automata. Given an alphabet A, we denote by $\mathcal{A} = (Q, I, T)$ an automaton with Q as set of states, I as set of initial states and T as set of terminal states. The automaton is defined by its set of edges $E \subset Q \times A \times Q$. The automaton is said to be *finite* if the set E is finite. A *path* in $\mathcal{A}$ is a sequence $p_0 \xrightarrow{a_1} p_1 \cdots \xrightarrow{a_n} p_n$ of consecutive edges. Its *label* is the word $w = a_1 \cdots a_n$. The path is *null* if the sequence is empty, that is if $w = 1$.

We denote by $L(\mathcal{A})$ the set of labels of paths from I to T. We say that $\mathcal{A}$ *recognizes* the set $L(\mathcal{A})$. A set $X \subset A^*$ is said to be *recognizable* if it can be recognized by a finite automaton.

The automaton $\mathcal{A} = (Q, I, T)$ is *trim* if for any state $q \in Q$, there is a path from I to q and from q to T. An automaton is called *simple* if

(i) it is trim,

(ii) there is a unique initial state, a unique terminal state and they are equal.

Let $\mathcal{A} = (Q, 1, 1)$ be a simple automaton. A path $p \xrightarrow{w} q$ in $\mathcal{A}$ is said to be *simple* if it is not the null path (that is $w \neq 1$) and if for any factorization $p \xrightarrow{u} r \xrightarrow{v} q$ of the path into nonnull paths, one has $r \neq 1$.

We denote by $\varphi_{\mathcal{A}}$ the morphism from A^* into the monoid of relations on the set Q defined by $\varphi_{\mathcal{A}}(w) = \{(p, q) \in Q \times Q \mid p \xrightarrow{w} q\}$. For a word w, we will often talk of $\varphi_{\mathcal{A}}(w)$ as the relation on Q defined by w. The monoid $M = \varphi_{\mathcal{A}}(A^*)$ is a monoid of relations on Q which is called the *transition monoid* of the automaton $\mathcal{A}$. We denote by 1 the identity relation and by 0 the empty relation.

An automaton $\mathcal{A} = (Q, I, T)$ is *deterministic* if it has a unique initial state and for any $p \in Q$ and $a \in A$, there is at most one $q \in Q$ such that (p, a, q) is an edge of $\mathcal{A}$.

For any set $X \subset A^+$ the *minimal automaton* of X is the deterministic automaton $\mathcal{A} = (Q, i, T)$ defined as follows. The elements of Q are the classes of the equivalence on A^* defined by $u \equiv v$ if for any $w \in A^*$, one has $uw \in X$ if and only if $vw \in X$. For each $a \in A$ there is an edge with label a from the class of a word u to the class of ua. The initial state is the class of the empty word. The terminal states are the classes included in X. The transition monoid of the minimal automaton is the *syntactic monoid* of X.

The automaton is *unambiguous* if for any $p, q \in Q$ and $w \in A^*$ there is at most one path from p to q labeled w. A deterministic automaton is clearly unambiguous.

For any code $X \subset A^+$, there exists a simple unambiguous automaton recognizing X^*. It can be obtained as follows. Let $\mathcal{A} = (Q, I, T)$ be a trim unambiguous automaton recognizing X. Let E be the set of edges of $\mathcal{A}$. Let $\omega \notin Q$ be a new state. Let $\mathcal{B} = (Q \cup \omega, \omega, \omega)$ be the automaton with edges formed of the edges of $\mathcal{A}$ plus the edges (ω, a, q) such that $(i, a, q) \in E$ for some $i \in I$, the edges (p, a, ω) such that $(p, a, t) \in E$ for some $t \in T$ and the edges (ω, a, ω) such that $(i, a, t) \in E$ for some $i \in I$ and $t \in T$. Then the trim part of $\mathcal{B}$ is a simple unambiguous automaton denoted $\mathcal{A}^*$ which recognizes X^*. Moreover, X is the set of labels of simple paths in $\mathcal{A}^*$.

When X is prefix, provided the automaton $\mathcal{A}$ is deterministic, the automaton $\mathcal{A}^*$ is also deterministic. Moreover, the minimal automaton of X^* is simple.

Unambiguous monoids of relations. Let m be a relation between two sets P and Q and let n be a relation between two sets Q and R. The product mn is *unambiguous* if for any $(p, r) \in P \times R$ there is at most one $q \in Q$ such that $(p, q) \in m$ and $(q, r) \in n$. A monoid M of relations on a set Q is *unambiguous* if for any $m, n \in M$ the product mn is unambiguous. When $\mathcal{A}$ is an unambiguous automaton, the monoid $M = \varphi_{\mathcal{A}}(A^*)$ is unambiguous.

A monoid M of relations on a set Q is *transitive* if for any $p, q \in Q$ there exists an element $m \in M$ such that $(p, q) \in m$ (note that this term is in agreement with the notion of a transitive permutation group).

The *rank* of a relation m between sets P and Q is the minimal cardinality of a set R for which there exist relations u on $P \times R$ and v on $R \times Q$ such that $m = uv$ and such that the product uv is unambiguous. Thus, the rank of m is zero if and only if m is the empty relation.

Let M be a transitive unambiguous monoid of relations containing relations of finite rank and not containing the empty relation. Let $r(M)$ be the minimal rank of the elements of M. The set of relations of rank $r(M)$ is the *minimal ideal* of M (see [1] Theorem 9.3.15). It is the intersection of all the ideals of M.

Let M be an unambiguous monoid of relations on a set Q. We denote by $\mathrm{Fix}(m)$ the set of fixpoints of an element $m \in M$. It is the set of $q \in Q$ such that $(q, q) \in m$. The rank of an idempotent is equal to the number of its fixpoints (see [1], Proposition 9.3.6).

The following characterization of idempotents is useful (see [1] for more details).

Lemma 3 *Let M be an unambiguous monoid of relations on a set Q. An element $m \in M$ is idempotent if and only if the following condition is satisfied: For any $p, q \in Q$, one has $(p, q) \in m$ if and only if there is a fixpoint r of m such that $(p, r), (r, q) \in m$.*

Proof. The condition is sufficient. Indeed, it implies directly that $m \subset m^2$. Conversely, suppose that $(p, q) \in m^2$. Let $r \in Q$ be such that $(p, r), (r, q) \in m$. By the condition, there are $s, t \in \mathrm{Fix}(m)$ such that $(p, s), (s, r), (r, t), (t, q) \in m$. Thus we have $(p, r), (p, t) \in m^2$ and $(r, q), (t, q) \in m$. By unambiguity, this implies $r = t$. Thus $r \in \mathrm{Fix}(m)$ and (p, q) is in m by the condition.

Conversely, suppose that m is idempotent. Let $p, q \in Q$ be such that $(p, q) \in m$. Since $m = m^3$, there exist $r, s \in Q$ such that $(p, r), (r, s), (s, q) \in m$. Since $m = m^2$ we have also $(r, q) \in m$ and $(p, s) \in m$. By unambiguity, we obtain $r = s$ and thus $r \in \mathrm{Fix}(m)$. ∎

Let M be an unambiguous monoid of relations on a set Q. Let $G \subset M$ be a group in M and let e be the neutral element of G. The group G is faithfully represented as a permutation group on the set $R = \mathrm{Fix}(e)$. This means that the restriction of the elements of G to $R \times R$ is an isomorphism from G onto a permutation group on R. We will often, by abuse of notation, identify the group G with this permutation group (although the elements of G are relations on Q). Since $\mathrm{Card}(R)$ is equal to the rank of e, the group G is a a permutation group of degree equal to the rank of e.

For $r \in \mathrm{Fix}(e)$ and $g \in G$, we denote by rg the image of r by the permutation defined by g on R. It is the unique fixpoint $s \in R$ such that $(r, s) \in g$. Thus the permutation defined by g on R is the restriction of the relation g to $R \times R$. It is thus contained in the relation g.

For an unambiguous automaton $\mathcal{A}$ on a set Q of states and a word w, we say that w *contains* a permutation π on $R \subset Q$ if π is the restriction of $\varphi_{\mathcal{A}}(w)$ to $R \times R$. When R is finite and is the set of fixpoints of an idempotent e, the permutation π is an element of the maximal group G containing e. Set indeed $m = e\varphi_{\mathcal{A}}(w)e$. Then $em = me = m$. Moreover, since R is finite there is an integer $k \geq 1$ such that the restriction to R of m^k is the identity and thus $m^k = e$. This shows that m^{k-1} is the inverse of m in G.

Let M be a transitive unambiguous monoid of relations not containing the empty relation. Let I be the minimal ideal of M, which is formed of the elements of M of rank $r(M)$. The set I is a union of equivalent transitive groups of degree $r(M)$ (see [1], Theorem 9.3.15). The *Suschkevitch group* of M is any of them.

Let $X \subset A^+$ be a code and let $\mathcal{A}$ be a simple unambiguous automaton recognizing X^*. Some of the groups in $\varphi_{\mathcal{A}}(A^*)$ do not depend on the choice of the unambiguous automaton. Indeed, let F be the set of factors of the words of X. If $\mathcal{A}$ and $\mathcal{B}$ are two simple unambiguous automata such

that $X^* = L(\mathcal{A}) = L(\mathcal{B})$, any group contained in $\varphi_{\mathcal{A}}(A^* \setminus F)$ is equivalent to a group in $\varphi_{\mathcal{B}}(A^* \setminus F)$ (see [1], Proposition 9.5.1). In particular, this is true for the group $G(X)$ of the code X, which is the Suschkevitch group of the monoid of transitions of any simple unambiguous automaton recognizing X^* (see [1], Proposition 9.5.2).

We will use later the following elementary results (see [1]). The first one is a property of unambiguous automata.

Proposition 1 *Let $X \subset A^+$ be a code and let $\mathcal{A}$ be a simple unambiguous automaton recognizing X^*. Let G be a group which meets $\varphi_{\mathcal{A}}(X^*)$. Then $G \cap \varphi_{\mathcal{A}}(X^*)$ is a subgroup of G.*

Proof. We use the fact that the submonoid $N = \varphi_{\mathcal{A}}(X^*)$ is stable. Indeed, let u be in $G \cap \varphi_{\mathcal{A}}(X^*)$. Let e be the neutral element of G. Then $ue = eu = u$ implies that $e \in N$. Next, if v is the inverse of u in G, then $uv, vu \in N$ imply $v \in N$. Thus $G \cap N$ is a subgroup of G. ∎

The second one is a classical property of monoids.

Proposition 2 *Let G be a group in a monoid M. Let $m, n \in M$ be such that $mn \in G$. Then nGm is a group isomorphic to G.*

Proof. Since $mn \in G$, we have $nGmnGm \subset nGm$. Next $e = n(mn)^{-1}m \in nGm$ is an idempotent. Thus nGm is a monoid. For any $g \in G$, the element $h = n((mn)^{-1}g^{-1}(mn)^{-1})m$ is the inverse of ngm. Thus nGm is a group and finally, the map $f : G \to nGm$ defined by $f(g) = n(mn)^{-1}gm$ is an isomorphism from G onto nGm. ∎

3 Main result

We will prove the following result.

Theorem 1 *Let $X \subset A^+$ be a code with empty kernel and let F be the set of internal factors of the words of X. Let $\mathcal{A}$ be a simple unambiguous automaton recognizing X^*. Any group contained in $\varphi_{\mathcal{A}}(A^* \setminus F)$ is a finite cyclic group which is regular.*

Observe that that since $\varphi_{\mathcal{A}}(A^* \setminus F)$ is an ideal, for a group G contained in $\varphi_{\mathcal{A}}(A^*)$, the condition $G \subset \varphi_{\mathcal{A}}(A^* \setminus F)$ is equivalent to $G \cap \varphi_{\mathcal{A}}(A^* \setminus F) \neq \emptyset$. Observe also that the groups above are not always transitive (see Example 8). Before giving the proof, we list some corollaries. The following statement is the result appearing at the end of [5] with an incorrect proof.

Corollary 1 *Let $X \subset A^+$ be a semaphore code and let F be the set of internal factors of the words of X. Let $\mathcal{A}$ be a simple deterministic automaton recognizing X^*. Any group contained in $\varphi_{\mathcal{A}}(A^* \setminus F)$ is a finite cyclic group which is regular.*

Proof. The result follows directly from Theorem 1 since a semaphore code has empty kernel. ∎

The second corollary concerns the group $G(X)$ which is a finite transitive permutation group for any thin complete code (thus the fact that such a group is cyclic implies that it is regular).

Corollary 2 *Let X be a semaphore code. Then the group $G(X)$ is cyclic.*

Proof. Let F be the set of internal factors of the words of X. Let $\mathcal{A}$ be a simple deterministic automaton recognizing X^*. Set $\varphi = \varphi_{\mathcal{A}}$ and $M = \varphi(A^*)$. Since X is a semaphore code, it is thin and complete. Thus M has elements of finite rank and does not contain the empty relation (see [1], Theorem 9.4.1). Let e be an idempotent of minimal rank in M. Since the minimal ideal of M is the set of elements of minimal rank, e belongs to the minimal ideal. Then $G = eMe$ is the maximal group containing e. Thus it is the Suschkevitch group of the monoid M. Since the elements of G belong to the minimal ideal of M, the group G is contained in the ideal $\varphi(A^* \setminus F)$ and the result follows. ∎

Corollary 3 *Let $X \subset A^+$ be a finite code with empty kernel. Let $\mathcal{A}$ be a simple unambiguous automaton recognizing X^*. Then any group in $\varphi_{\mathcal{A}}(A^*)$ is cyclic and regular.*

Proof. Let F be the set of internal factors of the words of X and let $M = \varphi_{\mathcal{A}}(A^*)$. Since X is finite, the ideal $\varphi_{\mathcal{A}}(A^* \setminus F)$ contains any group G distinct from 1 in M and the result follows. ∎

The following lemma is used in the proof of Theorem 1.

Lemma 4 *Let $X \subset A^+$ be a code and let F be the set of internal factors of words in X. Let $\mathcal{A} = (Q, 1, 1)$ be a simple unambiguous automaton recognizing X^*. Let G be a group contained in $\varphi_{\mathcal{A}}(A^* \setminus F)$, let e be the neutral element of G and let $R = \mathrm{Fix}(e)$ be the set of fixpoints of e. For any $g \in G$, any word $w \in \varphi_{\mathcal{A}}^{-1}(g) \setminus F$ and each $r \in R$, there is a unique interpretation α_r of w such that there are paths $r \xrightarrow{s_{\alpha_r}} 1$ and $1 \xrightarrow{p_{\alpha_r}} rg$ which are simple or null. Moreover, the set $I = \{\alpha_r \mid r \in R\}$ is formed of independent interpretations.*

Proof. For each $r \in R$, there is a path $r \xrightarrow{w} rg$. Since $\mathcal{A}$ is trim, there exist $f, h \in A^*$ such that $1 \xrightarrow{f} r$ and $rg \xrightarrow{h} 1$. Since $w \notin F$, there exists an interpretation α_r of w such that $r \xrightarrow{s_{\alpha_r}} 1$ and $1 \xrightarrow{p_{\alpha_r}} rg$ are simple or null paths. This interpretation is clearly unique.

The interpretations α_r, for $r \in R$, are independent. Suppose indeed that for $r, s \in R$ there are $u, v \in A^*$ and $x \in X^*$ such that $w = uxv$, $u \in P(\alpha_r)$ and $ux \in P(\alpha_s)$. Then we have the paths $r \xrightarrow{u} 1 \xrightarrow{xv} rg$ and $s \xrightarrow{ux} 1 \xrightarrow{v} sg$, which imply the existence of a path $r \xrightarrow{u} 1 \xrightarrow{x} 1 \xrightarrow{v} sg$ (see Figure 6). This means that $(r, sg) \in g$ contradicting the fact that g is a permutation on R.

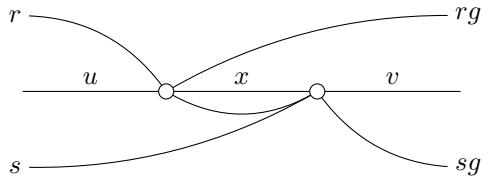

Figure 6: The interpretations α_r and α_s are independent.

∎

Proof of Theorem 1. Set $\mathcal{A} = (Q, 1, 1)$, and $\varphi = \varphi_{\mathcal{A}}$. Let G be a group contained in $\varphi(A^* \setminus F)$ and let e be the neutral element of G. We first show that one may assume that G meets $\varphi(X^*)$.

We may suppose that G is not reduced to the empty relation since otherwise the group G is trivial and there is nothing to prove. Let $w \in \varphi^{-1}(e) \setminus F$. Since e is an idempotent which is not

the empty relation, it has at least one fixpoint q. Since the automaton $\mathcal{A}$ is trim, there are words $u, v \in A^*$ such that $1 \xrightarrow{u} q$ and $q \xrightarrow{v} 1$. Then uwv is in X^*. Since $w \notin F$, there exist $t, z \in A^*$ such that $w = tz$ with $ut, zv \in X^*$. Then $q \xrightarrow{t} 1$ and $1 \xrightarrow{z} q$ and thus $zt \in X^*$. The set $\varphi(z)G\varphi(t)$ is a group isomorphic to G by Proposition 2. It meets $\varphi(X^*)$ since $\varphi(z)e\varphi(t) = \varphi(ztzt) \in \varphi(X^*)$. This shows that we may assume G meets $\varphi(X^*)$.

Since G meets $\varphi(X^*)$, the intersection $G \cap \varphi(X^*)$ is a subgroup by Proposition 1. This implies that $e \in \varphi(X^*)$. Let $w \in \varphi^{-1}(e) \setminus F$. Thus $w \in X^*$. Let $R = \mathrm{Fix}(e)$. Since $e \in \varphi(X^*)$, we have $1 \in R$. By Lemma 4, the word w has a set I of independent interpretations α_r for $r \in R$ such that $r \xrightarrow{s_{\alpha_r}} 1$ and $1 \xrightarrow{p_{\alpha_r}} r$ are simple or null paths. Set $s_r = s_{\alpha_r}$, $f_r = f_{\alpha_r}$, $x_r = c(f_r)$ and $p_r = p_{\alpha_r}$ (see Figure 7).

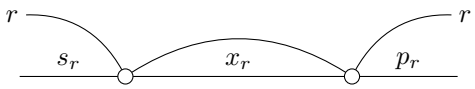

Figure 7: The interpretation α_r.

The map $r \mapsto s_r$ is injective since the interpretations are disjoint. This implies that R is finite and thus that G is finite.

Set $R = \{1, 2, \ldots, n\}$. We may suppose that s_i is a proper prefix of s_{i+1} for $1 \leq i < n$. We are going to prove that all elements of G are powers of the permutation $\alpha = (1\ 2 \cdots n)$. This implies our conclusion since a subgroup of a cyclic and regular group is also cyclic and regular.

Denote by $\gamma = (v_1, v_2, \ldots, v_\ell)$ the supremum of the interpretations α_i of w. Since $s_1 = p_1 = 1$, we have $v_1 = v_\ell = 1$. For $1 \leq i \leq n$, set $w = s_i x_i p_i$ with $x_i = c(f_i)$. We have

$$s_i = v_1 \cdots v_i, \quad x_i = v_{i+1} \cdots v_j \text{ and } p_i = v_{j+1} \cdots v_\ell \tag{4}$$

with $1 \leq i \leq j < \ell$. Then, by Lemma 2, γ is n-periodic. Since $w \in X^*$ and $x_i \in X^*$, Equation (3) implies

$$j - i \equiv \ell - 2 \equiv 0 \mod n. \tag{5}$$

Consider an element $g \in G$ and a word $z \in \varphi^{-1}(g)$. Then $\varphi(wzw) = g$. Since $g \in G$, by Lemma 4 the word wzw has a set J of n independent interpretations β_i such that $i \xrightarrow{s_{\beta_i}} 1$ and $1 \xrightarrow{p_{\beta_i}} ig$ are simple or null paths.

The path $i \xrightarrow{w} i \xrightarrow{z} ig \xrightarrow{w} ig$ decomposes as

$$i \xrightarrow{s_i} 1 \xrightarrow{x_i} 1 \xrightarrow{p_i} i \xrightarrow{z} ig \xrightarrow{s_{ig}} 1 \xrightarrow{x_{ig}} 1 \xrightarrow{p_{ig}} ig.$$

Thus the sequence $(s_i, x_i p_i z s_{ig} x_{ig}, p_{ig})$ is an interpretation of wzw. Since the paths $i \xrightarrow{s_i} 1$ and $1 \xrightarrow{p_{ig}}$ are simple or null, this implies by uniqueness of β_i that $s_{\beta_i} = s_i$, $c(f_{\beta_i}) = x_i p_i z s_{ig} x_{ig}$ and $p_{\beta_i} = p_{ig}$ for $1 \leq i \leq n$ (see Figure 8). In particular, we have for each $i \in R$, $p_i z s_{ig} \in X^*$.

The supremum of the interpretations β_i is of the form

$$\delta = (v_1, v_2, \ldots, v_{\ell-1}, u_1, u_2, \ldots, u_m, v_2, \ldots, v_\ell)$$

for some $m > 0$ and some nonempty words $u_1, \ldots, u_m$ such that $z = u_1 \cdots u_m$. Indeed, the first $\ell - 1$ terms of γ and δ coincide and the term of index ℓ of δ is u_1 instead of v_ℓ which is empty.

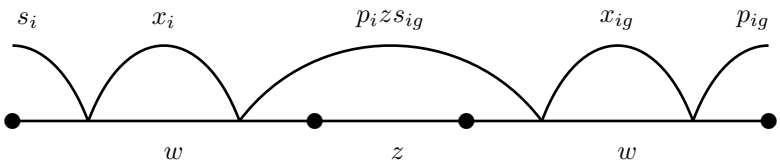

Figure 8: An interpretation of wzw.

Similarly, the last $\ell - 1$ terms of γ and δ coincide and the term of index m of δ is u_m instead of v_1 which is empty.

We then have for $1 \leq i \leq n$, by Equation (4),

$$p_i z s_{ig} = v_{j+1} \cdots v_{\ell-1} u_1 \cdots u_m v_2 \cdots v_{ig}.$$

Thus, since $c(f_{\beta_i}) = x_i p_i z s_{ig} x_{ig}$, we obtain, with the functions λ, μ, ν defined in (2),

$$\mu(\beta_i, J) = \mu(\alpha_i, I) + \nu(\alpha_i, I) + m + \lambda(\alpha_{ig}, I) + \mu(\alpha_{ig}, I).$$

Since $\mu(\alpha_i, I) \equiv \mu(\alpha_{ig}, I) \equiv 0 \mod n$, we obtain $\mu(\beta_i, J) \equiv \ell - j - 1 + m + ig - 1 \mod n$. Since δ is n-periodic, we have $\ell - j - 1 + m + ig - 1 \equiv 0 \mod n$. Since $\ell \equiv 2 \mod n$ and $i \equiv j \mod n$ by Equation (5), this implies that $-i + m + ig \equiv 0 \mod n$. Thus $ig \equiv i - m \mod n$. Since this holds for $1 \leq i \leq n$, we conclude that $g = \alpha^{-m}$. This shows that G is included in the cyclic group generated by α and thus that G is cyclic and regular. ∎

Note that the permutation α of the above proof is not necessarily in G. This is the difficulty: the group G is cyclic but it has no obvious generator (see Example 8).

4 Examples

We illustrate the results on a series of examples.

The next three examples give instances of cyclic groups in the syntactic monoid of X^* for a finite code $X \subset A^+$ with empty kernel on the alphabet $A = \{a, b\}$. Note that when the code is finite, by Corollary 3, all groups are cyclic and we do not have to distinguish between groups contained in $\varphi(F)$ and groups contained in $\varphi(A^* \setminus F)$.

Example 6 Let $X = \{aa, bb, baa, bba\}$. The set X is a code with empty kernel. A simple unambiguous automaton recognizing X^* is shown in Figure 9. The word a contains the cycle (12) and the word b the cycle (13).

Example 7 Let $X = \{aa, aba, bab, bb\}$. The set X is an infix code. The minimal automaton $\mathcal{A}$ of X^* is represented in Figure 10.

The transition monoid M of $\mathcal{A}$ contains groups which are cyclic of order 1, 2 or 3. For example, ab contains the cycle (134) while a contains the cycle (12). Let us note an interesting feature of

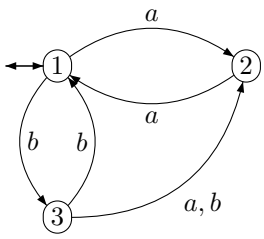

Figure 9: A code with empty kernel defining cyclic groups of order 2.

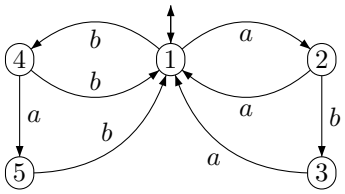

Figure 10: An infix code defining cyclic groups of degree (and order) 2 and 3.

this example. Let G be the cyclic group of order 2 formed by the images of aa and aaa in M. The set $\varphi^{-1}(G)$ is a submonoid which is not cyclic. It is not even finitely generated. Indeed, Figure 11 shows that any word w in $(a \cup babb^*aba)^*$ fixes globally the set $\{1, 2\}$ and thus is such that $\varphi(a^2wa^2) \in G$.

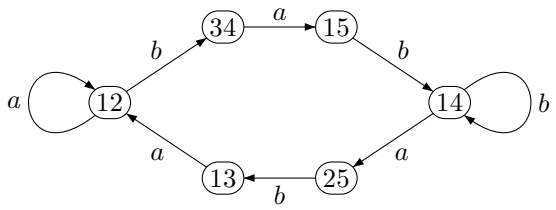

Figure 11: The action of A^* on the 2-element subsets reachable from $\{1, 2\}$

Example 8 Let $X = \{aaa, aab, abaa, abab, baba, babb, bba, bbb\}$. The set X is an infix code. The minimal automaton $\mathcal{A}$ of X^* is represented in Figure 12. The transition monoid $M = \varphi(A^*)$ of $\mathcal{A}$ contains cyclic groups of degree 1, 2, 3 and 4. For example the word a contains the cycle (123). In turn, ba contains the permutation (16)(23). This example shows another interesting feature. Consider the group G containing $\varphi(ba)$. The neutral element of G is $e = \varphi(baba)$ and its set of fixpoints is $\{1, 2, 3, 6\}$. The group G is of degree 4. It is composed of the permutation (16)(23) and the identity. It is thus of order 2. The permutation α of the proof of Theorem 1 is (1362) (see Figure 13). It does not belong to G. Actually, M does not contain any cyclic group of order 4.

Let us mention an interesting case where the hypothesis of the above theorem are satisfied. Let G be a transitive permutation group on $R = \{1, 2, \ldots, n\}$ and let $\varphi : A^* \to G$ be a surjective morphism. Let H be the subgroup of G which fixes 1. Let Z be the bifix code generating the submonoid $\varphi^{-1}(H)$. Let X be the set of elements of Z which have no proper factor in Z.

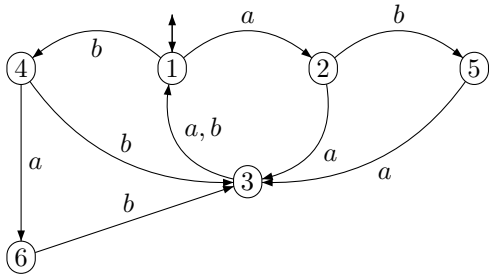

Figure 12: An infix code with a group of degree 4 and order 2.

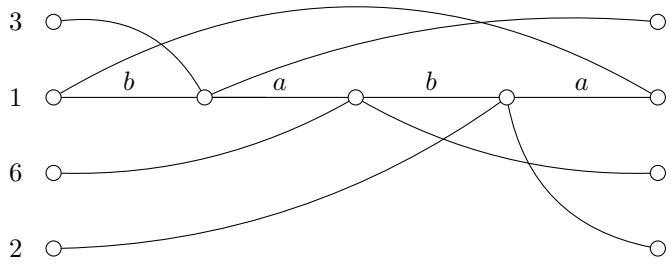

Figure 13: The interpretations of *baba*.

Proposition 3 *The set X is a finite infix code. The groups in the syntactic monoid M of X^*, not reduced to the neutral element of M, are cyclic of degree at most n.*

Proof. The set X is clearly an infix code. To prove that X is finite, consider a word z of Z of length at least equal to $n+2$. Since z has at least $n+1$ nonempty proper suffixes, there exist two distinct nonempty proper suffixes u, v of z such that $1\varphi(u) = 1\varphi(v)$. We may suppose that u is shorter than v. Then $v = wu$ with $1\varphi(w) = 1\varphi(v)\varphi(u)^{-1} = 1$ and thus $w \in Z^+$. This shows that $z \notin X$. This implies that the words in X have length at most $n+1$ and thus that X is finite.

Let M be the syntactic monoid of X^* and let $\mathcal{A}$ be the minimal automaton of X^*. By definition, we have $M = \varphi_{\mathcal{A}}(A^*)$.

Let G' be a group contained in M not reduced to the neutral element of M. Let e be the neutral element of G'. By Corollary 3, G' is cyclic and regular. The degree of G' is equal to the rank of e.

Since $G' \neq 1$, the set $\varphi^{-1}(e)$ contains nonempty words. Since it is a submonoid, it contains words of arbitrary large length. In particular, $\varphi^{-1}(e)$ contains words of length larger than the length of any word in X and thus words which are not factor of a word in X. Let w be a word in $\varphi_{\mathcal{A}}^{-1}(e)$ which is not a factor of a word in X. For any fixpoint p of e, there is an interpretation α of w with respect to X such that $p \xrightarrow{s_\alpha} 1$ and $1 \xrightarrow{p_\alpha} p$. The interpretations corresponding to distinct fixpoints are distinct (and even independent). Since $X \subset Z$, these interpretations of w are also interpretations with respect to Z.

The number of interpretations of w with respect to Z is at most equal to n. Indeed, for each

interpretation α of w with respect to Z, there is a unique $r = r(\alpha) \in R$ such that $r\varphi(s_\alpha) = 1$. Since the map $\alpha \mapsto r(\alpha)$ is injective, the number of interpretations α is at most n.

Thus w cannot have more than n interpretations with respect to X. This implies that the number of fixpoints of e is at most n and the degree of G' is also at most n. ∎

Example 9 Let G be the symmetric group on the set $R = \{1, 2, 3\}$ and let $A = \{a, b\}$. Let $\varphi : A^* \to G$ be the morphism defined by $\varphi(a) = (12)$, $\varphi(b) = (13)$. The bifix code Z is the infinite set represented on the left of Figure 14. The code X corresponding to the above construction is

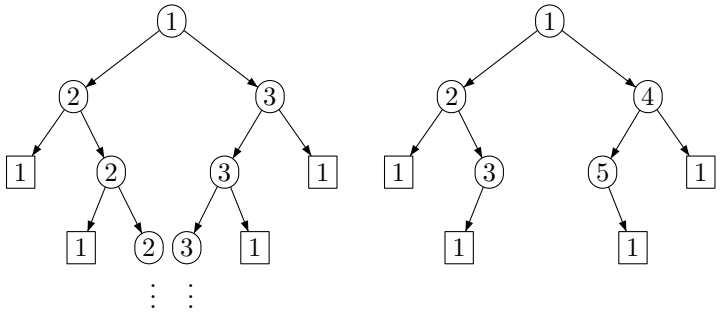

Figure 14: The infinite group code Z and the finite code X

represented on the right of Figure 14. It is the code of Example 7.

Example 10 The code X of Example 8 corresponds to the above construction with G being the symmetric group on the set $\{1, 2, 3, 4\}$ and $\varphi(a) = (123)$, $\varphi(b) = (143)$.

Example 11 Let us consider the morphism from $\{a, b\}^*$ to the symmetric group on $\{1, 2, 3, 4, 5\}$ defined by $\varphi(a) = (123)$, $\varphi(b) = (145)$. Then

$$X = \{aaa, aaba, aabba, abaa, ababa, abbaa, baabb, babab, babb, bbaab, bbab, bbb\}.$$

The transitions of the minimal automaton $\mathcal{A}$ of X^* are represented in Figure 15. The monoid M has 14351 elements. It contains cyclic groups of degrees from 1 to 5 and orders $1, 2, 3, 5$. The word ab contains the cycle (1 6 11 4 9) of length 5 and $(ab)^2$ has rank 5 (there is a second $\mathcal{D}$-class of elements of degree 5 containing the image of a^2b^2). The word $a^2ba^2b^2$ contains the permutation (1 12)(5 11) of degree 4 but there is no cyclic group of order 4 in M. The words a and b contains cycles of degree 3. The word a^4ba^5 contains the identity on $\{1, 2\}$ while the word $a^2bab^2a^2ba^4$ contains the transposition (1 2).

	1	2	3	4	5	6	7	8	9	10	11	12	13
a	2	3	1	8	9	7	1	13	10	−	1	11	−
b	4	6	7	5	1	12	11	9	1	1	−	−	10

Figure 15: The transitions of $\mathcal{A}$

5 Complements

We first show in the following example that Theorem 1 becomes false for groups which do not meet the ideal $\varphi_{\mathcal{A}^*}(A^* \setminus F)$ and that the transition monoid of a simple unambiguous automaton recognizing X^* may contain any finite or infinite group.

Example 12 Let G be a transitive permutation group on a set R and let $\varphi : A^* \to G$ be a surjective morphism. Let 1 be an element of R and let H be the subgroup of G formed by the permutations fixing 1. Let Z be the bifix code such that $Z^* = \varphi^{-1}(H)$. Let $\mathcal{B} = (R, 1, 1)$ be the deterministic automaton recognizing Z^* with edges $(p, a, p\varphi(a))$ for $p \in R$ and $a \in A$. Let $B = A \cup b$ where $b \notin A^*$ is a new letter. Then $X = bZ^*b$ is an infix code. Let $\mathcal{A} = (Q, i, i)$ be the automaton obtained from $\mathcal{B}$ adding a state $i \notin R$ and the two edges $(i, b, 1), (1, b, i)$. Then $\mathcal{A}$ is a simple unambiguous automaton recognizing X^*. Moreover G is isomorphic to a group contained in the transition monoid of $\mathcal{A}$. It is formed of the images in $M_{\mathcal{A}}$ of the words in A^* acting as a permutation group (identical to G) on the elements of R.

We now prove the following result concerning the groups which do not satisfy the hypothesis of Theorem 1. We denote by $M_{\mathcal{A}}$ the transition monoid of an automaton $\mathcal{A}$.

Proposition 4 *Let $X \subset A^+$ be a code with empty kernel and let F be the set of internal factors of the words of X. Let $\mathcal{A} = (Q, I, T)$ be a trim unambiguous automaton recognizing X. Any group H in $M_{\mathcal{A}^*}$ such that $\varphi_{\mathcal{A}^*}^{-1}(H) \subset F$ is isomorphic to a group in $M_{\mathcal{A}}$.*

Note that this statement is false if the kernel of X is nonempty, as shown in the following example.

Example 13 Let $X = a^2 \cup ba^*b$ and let $\mathcal{A}$ be the automaton represented on Figure 16 with $\mathcal{A}^*$ on the right. The monoid $M_{\mathcal{A}}$ contains only trivial groups. On the contrary, the set $G = \varphi_{\mathcal{A}^*}(a^*)$

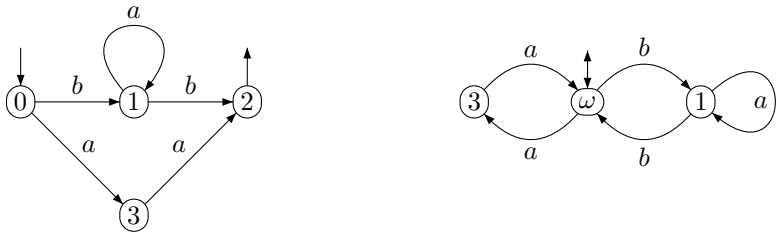

Figure 16: The automata $\mathcal{A}$ and $\mathcal{A}^*$.

is a cyclic group of order 2 such that $\varphi_{\mathcal{A}^*}^{-1}(G) \subset F$.

We will use the following technical lemma.

Lemma 5 *Let X be a code with empty kernel and let F be the set of internal factors of the words of X. Let $\mathcal{A}$ be a trim unambiguous automaton recognizing X. Let w be a nonempty word such that $w^* \subseteq F$. Then:*

1. $w^* \cap A^*XA^* = \emptyset$,

2. *a path* $p \xrightarrow{w} q$ *in the automaton* $\mathcal{A}^*$ *can pass at most once by* ω,

3. *no path* $r \xrightarrow{w} r$ *in the automaton* $\mathcal{A}^*$ *can pass by* ω,

4. $Fix(\varphi_{\mathcal{A}}(w)) = Fix(\varphi_{\mathcal{A}^*}(w))$.

Proof 1. No power of w can have a factor in X. Indeed, if w^n has a factor $x \in X$, then $x \in F$ and thus belongs to the kernel of X. This proves the first assertion.
2. A path labeled by w can pass at most once by ω since otherwise it would have a factor in X.
3. Follows from 2 since, otherwise, the path $r \xrightarrow{w} r \xrightarrow{w} r$ in $\mathcal{A}^*$ passes twice by ω.
4. All fixpoints of $\varphi_{\mathcal{A}}(w)$ are also fixpoints of $\varphi_{\mathcal{A}^*}(w)$ and, by assertion 3, $\varphi_{\mathcal{A}^*}(w)$ cannot have other fixpoints. ∎

Note that if a word w satisfies the hypotheses of Lemma 5, they are also satisfied by any power w^n with $n \geq 1$ of w. We prove a second technical lemma.

Lemma 6 *Let* $X \subset A^+$ *be a code with empty kernel and let* F *be the set of internal factors of the words of* X. *Let* $\mathcal{A} = (Q, I, T)$ *be a trim unambiguous automaton recognizing* X. *For a nonempty word* w *such that* $w^* \subset F$, *there is an idempotent in* $\varphi_{\mathcal{A}}(w^+)$ *if and only if there is one in* $\varphi_{\mathcal{A}^*}(w^+)$.

Proof.
1. Suppose first that $\varphi_{\mathcal{A}}(w^+)$ contains an idempotent. Changing w into some of its powers, we may assume that $e = \varphi_{\mathcal{A}}(w)$ is an idempotent of $M_{\mathcal{A}}$. Set $f = \varphi_{\mathcal{A}^*}(w)$. Let us show that $f^2 = f^3$, which implies that f^2 is idempotent. Suppose indeed that we have a path $p \xrightarrow{w^2} q$ in $\mathcal{A}^*$. If this path does not pass by ω, then it is a path in $\mathcal{A}$ and thus we have also $p \xrightarrow{w^3} q$. Otherwise, since w^2 does not have a factor in X by Lemma 5, it can have only one occurrence of ω. We may suppose that this occurrence is in the first half of the path. The other case is symmetrical. Thus, suppose that we have $w = uv$ with $p \xrightarrow{u} \omega$ and $\omega \xrightarrow{vw} q$. Then, since the path $\omega \xrightarrow{vw} q$ does not pass by ω except at its origin, there is a path $i \xrightarrow{vw} q$ in $\mathcal{A}$ for some $i \in I$. Since $e = \varphi_{\mathcal{A}}(w)$ is idempotent, we also have a path $i \xrightarrow{vw^2} q$ in $\mathcal{A}$ and consequently a path $\omega \xrightarrow{vw^2} q$ in $\mathcal{A}^*$. Finally, there is a path $p \xrightarrow{w^3} q$ in $\mathcal{A}^*$. This shows that $f^2 \subset f^3$.

To show the converse inclusion, consider a path $p \xrightarrow{w^3} q$ in $\mathcal{A}^*$. If this path does not pass by ω, then it is a path in $\mathcal{A}$ and thus we have also a path $p \xrightarrow{w^2} q$ in $\mathcal{A}$ and thus in $\mathcal{A}^*$. Otherwise, suppose first that there is a factorization $w = uv$ such that $p \xrightarrow{u} \omega \xrightarrow{vw^2} q$. Since ω does not have a second occurence on this path by Lemma 5, the path $\omega \xrightarrow{vw^2} q$ does not pass by ω except at its origin. Thus, there is a path $i \xrightarrow{vw^2} q$ in $\mathcal{A}$ for some $i \in I$. Since $e = \varphi_{\mathcal{A}}(w)$ is idempotent, there there is also a path $i \xrightarrow{vw} q$ in $\mathcal{A}$ and thus a path $\omega \xrightarrow{vw} q$ in $\mathcal{A}^*$. Thus there is also a path $p \xrightarrow{u} \omega \xrightarrow{vw} q$ in $\mathcal{A}^*$ which is a path $p \xrightarrow{w^2} q$. The case where there is a path $p \xrightarrow{w^2u} \omega \xrightarrow{v} q$ in $\mathcal{A}^*$ is similar. Finally, there cannot exist a path $p \xrightarrow{wu} \omega \xrightarrow{vw} q$ in $\mathcal{A}^*$ with $w = uv$. Indeed, since e is idempotent, we have also paths $p \xrightarrow{w^2} r \xrightarrow{u} \omega \xrightarrow{v} s \xrightarrow{w} q$ and $p \xrightarrow{w} r \xrightarrow{u} \omega \xrightarrow{v} s \xrightarrow{w^2} q$ for some $r, s \in Q$. By unambiguity, we obtain $r = s$ and thus the existence of a path $r \xrightarrow{u} \omega \xrightarrow{v} r$, which is impossible. This shows that $f^3 \subset f^2$.

2. Conversely, suppose that $f = \varphi_{\mathcal{A}^*}(w)$ is idempotent. Let $e = \varphi_{\mathcal{A}}(w)$. We show that $e^2 = e^3$, which implies that e^2 is idempotent. Consider first a path $p \xrightarrow{w^2} q$ in $\mathcal{A}$. Let $u, v \in A^*$ and $s \in Q$ be such that $i \xrightarrow{u} p \xrightarrow{w} s \xrightarrow{w} q \xrightarrow{v} t$ with $i \in I$ and $t \in T$.

By definition of $\mathcal{A}^*$, we also have a path $\omega \xrightarrow{u} p \xrightarrow{w} s \xrightarrow{w} q \xrightarrow{v} \omega$. Since $f = \varphi_{\mathcal{A}^*}(w)$ is idempotent with $(p, q) \in f$, by Lemma 3, there is a path $p \xrightarrow{w} r \xrightarrow{w} q$ in $\mathcal{A}^*$ with $r \in \mathrm{Fix}(f)$. By unambiguity we have $r = s$.

By Lemma 5 the path $s \xrightarrow{w} s$ does not pass by ω. Thus we also have a path $p \xrightarrow{w} s \xrightarrow{w} s \xrightarrow{w} q$ in $\mathcal{A}$ and finally a path $p \xrightarrow{w^3} q$.

This shows that $e^2 \subset e^3$. The converse inclusion is proved in the same way by reversing the implications. ∎

Note that Lemma 6 is obvious when the code X is recognizable and the automaton $\mathcal{A}$ is finite. Indeed, in this case, the monoids $M_{\mathcal{A}}$ and $M_{\mathcal{A}^*}$ are finite and in a finite monoid, any element has a power which is idempotent.

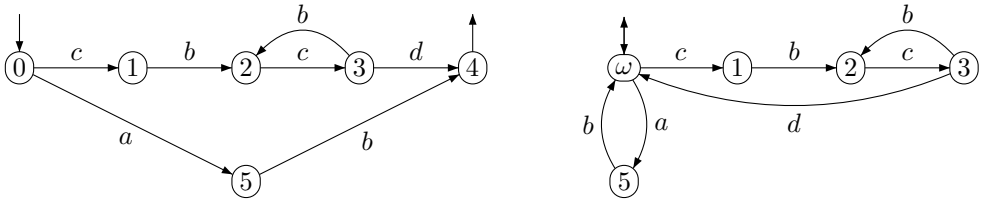

Figure 17: The automata $\mathcal{A}$ and $\mathcal{A}^*$ for $X = ab \cup (cb)^+cd$.

The following examples illustrate the proof of Lemma 6.

Example 14 Let $X = ab \cup (cb)^+cd$ which is a code with empty kernel on the alphabet $A = \{a, b, c, d\}$. A trim deterministic automaton $\mathcal{A}$ recognizing X and the corresponding automaton $\mathcal{A}^*$ are shown on Figure 17.

It is easy to verify that $e = \varphi_{\mathcal{A}}(bc)$ is idempotent while $f = \varphi_{\mathcal{A}^*}(bc)$ satisfies $f^2 = f^3$ (but f is not idempotent) illustrating point 1 in the proof of Lemma 6.

Example 15 Let $X = ab \cup abcd \cup (cb)^+cd$ which is a code with empty kernel on the alphabet $A = \{a, b, c, d\}$. A trim unambiguous automaton $\mathcal{A}$ recognizing X and the corresponding automaton $\mathcal{A}^*$ are shown on Figure 18. It is easy to verify that $f = \varphi_{\mathcal{A}^*}(bc)$ is idempotent while $e = \varphi_{\mathcal{A}}(bc)$ satisfies $e^2 = e^3$ (but e is not idempotent), thus illustrating point 2 in the proof of Lemma 6.

Proof of Proposition 4. Since the monoids $M_{\mathcal{A}}$ and $M_{\mathcal{A}^*}$ both contain the group reduced to the identity, we may discard the case of groups reduced to the identity of $M_{\mathcal{A}}$ or $M_{\mathcal{A}^*}$, and thus of groups G such that $\varphi_{\mathcal{A}^*}^{-1}(G) = 1$ or $\varphi_{\mathcal{A}}^{-1}(G) = 1$. Note that if $\varphi_{\mathcal{A}}^{-1}(G) \neq 1$, then $\varphi_{\mathcal{A}}^{-1}(g) \neq 1$ for any $g \in G$. The same holds for $\varphi_{\mathcal{A}^*}$. We may also discard the case of the group reduced to the empty relation in $M_{\mathcal{A}}$.

Let f be an idempotent in $M_{\mathcal{A}^*}$ such that $\varphi_{\mathcal{A}^*}^{-1}(f) \subset F$. We may assume that X is not empty and thus that $f \neq 0$. By the above discussion, we may assume $\varphi_{\mathcal{A}^*}^{-1}(f) \neq 1$. Let $w \in F$ be a

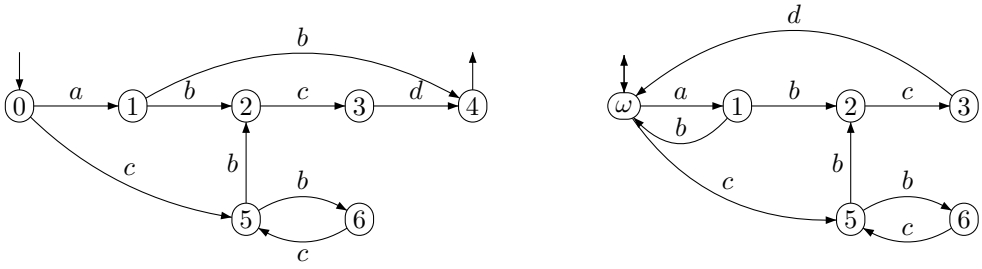

Figure 18: The automata $\mathcal{A}$ and $\mathcal{A}^*$ for $X = ab \cup abcd \cup (cb)^+cd$.

nonempty word in $\varphi^{-1}_{\mathcal{A}^*}(f)$. Since $\varphi_{\mathcal{A}^*}(w^+) = \{f\}$, by Lemma 6 there is an integer $n \geq 1$ such that $\varphi_{\mathcal{A}}(w^n)$ is an idempotent e of $M_{\mathcal{A}}$. By assertion 4 of Lemma 5 applied to w^n, the set of fixpoints of e and f are equal. Thus, in particular e is not the empty relation. We are going to prove that the maximal groups containing e and f respectively are isomorphic. This will prove the statement since any group in $M_{\mathcal{A}^*}$ is contained in a maximal group.

Set $R = \mathrm{Fix}(e) = \mathrm{Fix}(f)$. Let G be the maximal group in $M_{\mathcal{A}}$ containing e and H be the maximal group in $M_{\mathcal{A}^*}$ containing f. We are going to prove that G and H are equal as permutation groups on R. Let h be an element of H and let u be a nonempty word in $\varphi^{-1}_{\mathcal{A}^*}(h)$. Let v be a nonempty word in $\varphi^{-1}_{\mathcal{A}^*}(h^{-1})$. Then $\varphi_{\mathcal{A}^*}(uv) = f$. Let $r, s \in R$ be such that $r \xrightarrow{u} s$ in $\mathcal{A}^*$ and thus also $s \xrightarrow{v} r$. By Lemma 5 applied to uv, the path $r \xrightarrow{u} s$ cannot pass by ω since otherwise the path $r \xrightarrow{u} s \xrightarrow{v} r$ would pass by ω. Thus, we also have a path $r \xrightarrow{u} s$ in $\mathcal{A}$. This shows that G contains the permutation defined by h on R. Conversely, let g be an element of G and u, v be a nonempty words such that $\varphi_{\mathcal{A}}(u) = g$, $\varphi_{\mathcal{A}}(v) = g^{-1}$. Let $r, s \in R$ be such that there is a path $r \xrightarrow{u} s$ in $\mathcal{A}$. Since there is also a path $s \xrightarrow{v} r$ in $\mathcal{A}$, all states on the path $r \xrightarrow{u} s$ belong to the trim part of the automaton $\mathcal{B}$ used to build $\mathcal{A}^*$ (see the definition of $\mathcal{A}^*$ in Section 2.2). Thus they are states of $\mathcal{A}^*$. This shows that we also have a path $r \xrightarrow{u} s$ in $\mathcal{A}^*$ and proves that H contains the permutation g. Thus G and H are equal as permutation groups on R. ∎

Observe that it is not true in general that any idempotent $e \neq 0, 1$ in $M_{\mathcal{A}}$ is obtained as in the proof above from an idempotent $f \in M_{\mathcal{A}^*}$ such that $\varphi^{-1}_{\mathcal{A}^*}(f) \subset F$, as shown in the following example.

Example 16 Let $\mathcal{A}$ and $\mathcal{A}^*$ be the automata given in Figure 19. The automaton $\mathcal{A}$ is a trim de-

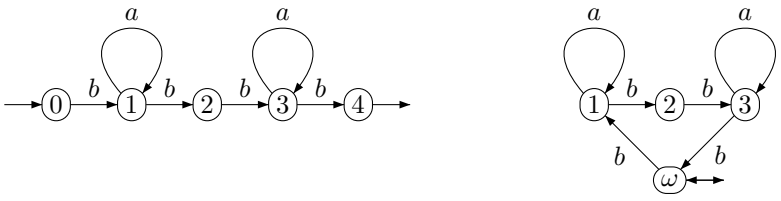

Figure 19: The automata $\mathcal{A}$ and $\mathcal{A}^*$

terministic automaton recognizing the code with empty kernel $X = ba^*bba^*b$. The set F of internal factors of X is the set of factors of a^*bba^*. Consider the idempotent $e = \varphi_{\mathcal{A}}(a)$. The idempotent $f = \varphi_{\mathcal{A}^*}(a)$ is not such that $\varphi_{\mathcal{A}^*}^{-1}(f) \subset F$. Indeed, the word $abba$ contains the permutation (13) and $\varphi_{\mathcal{A}^*}(abbaabba) = f$ although $abbaabba \notin F$.

We conclude with a consequence of the main result (Theorem 1) and of Proposition 4 concerning a closure property of a variety of finite monoids. Recall (see [2] for an introduction) that a *variety* of finite monoids is a class $\mathbf{V}$ of finite monoids which is closed under

(i) morphism: if $\varphi : M \to N$ is a morphism of monoids and $M \in \mathbf{V}$, then $N \in \mathbf{V}$,

(ii) submonoid: if $M \in \mathbf{V}$, any submonoid of M is in $\mathbf{V}$,

(iii) finite direct product: if $M, N \in \mathbf{V}$, then $M \times N \in \mathbf{V}$.

A variety of finite monoids is also called a *pseudovariety* of monoids, the name of a variety (in the sense of Birkhoff) being used when condition (iii) is replaced by the closure under arbitrary (possibly infinite) direct product. For simplicity, we use here the term of variety instead of pseudovariety.

The $*$-variety associated to a given variety $\mathbf{V}$ of finite monoids is, for each alphabet A, the family of recognizable sets $S \subset A^*$ such that the syntactic monoid of S belongs to the variety $\mathbf{V}$. Such a class is closed under boolean operations and residual: if $X \subset A^*$ is in $\mathcal{V}$ then for any $u \in A^*$, $u^{-1}X = \{v \in A^* \mid uv \in X\}$ and $Xu^{-1} = \{v \in A^* \mid vu \in X\}$ are in $\mathcal{V}$.

For any variety $\mathbf{G}$ of finite groups, the class of finite monoids containing only groups in $\mathbf{G}$ is a variety (see [2]). By a theorem of Schützenberger, the corresponding $*$-variety $\mathcal{V}$ is closed under product: if $X, Y \in \mathcal{V}$, then $XY \in \mathcal{V}$.

Let $\mathbf{V}$ be the variety of finite monoids containing only Abelian groups. Let $\mathcal{V}$ be the associated $*$-variety of sets. This variety has been studied by Schützenberger, who has described the $*$-variety $\mathcal{V}$ using another closure property (see [6] or [4]).

Theorem 2 *For any code X with empty kernel which belongs to $\mathcal{V}$, the set X^* is in $\mathcal{V}$.*

Proof. Let $\mathcal{A}$ be the minimal deterministic automaton of X. The transition monoid of $\mathcal{A}$ is the syntactic monoid of X and therefore is in the variety $\mathbf{V}$. The automaton $\mathcal{A}^*$ is a simple unambiguous automaton recognizing X^*. We show that the transition monoid M of $\mathcal{A}^*$ is in $\mathbf{V}$. Since the syntactic monoid of X^* is a quotient of M, this will prove that X^* is in $\mathcal{V}$. Let F be the set of internal factors of the words of X. Let G be a group contained in M. If G is contained in the ideal $\varphi_{\mathcal{A}^*}(A^* \setminus F)$, then G is cyclic by Theorem 1. Otherwise, by Proposition 4, G is isomorphic to a group contained in the transition monoid of $\mathcal{A}$ and thus G is Abelian. ∎

References

[1] Jean Berstel, Dominique Perrin, and Christophe Reutenauer. *Codes and Automata*. Cambridge University Press, 2009.

[2] Samuel Eilenberg. *Automata, languages, and machines. Vol. B.* Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. With two chapters ("Depth decomposition

theorem" and "Complexity of semigroups and morphisms") by Bret Tilson, Pure and Applied Mathematics, Vol. 59.

[3] Véronique Froidure and Jean-Eric Pin. Algorithms for computing finite semigroups. In *Foundations of computational mathematics (Rio de Janeiro, 1997)*, pages 112–126. Springer, Berlin, 1997.

[4] Gérard Lallement. *Semigroups and combinatorial applications*. John Wiley & Sons, New York-Chichester-Brisbane, 1979. Pure and Applied Mathematics, A Wiley-Interscience Publication.

[5] Marcel-Paul Schützenberger. On the synchronizing properties of certain prefix codes. *Inform. and Control*, 7:23–36, 1964.

[6] Marcel-Paul Schützenberger. Sur les monoides finis dont les groupes sont commutatifs. *Rev. Française Automat. Informat. Recherche Opérationnelle Sér. Rouge*, 8(R-1):55–61, 1974.

[7] Helmut Wielandt. *Finite permutation groups*. Academic Press, New York, 1964.